IN THE CLAIMS

Please cancel claim 11 without prejudice and subject to Applicant's right to prosecute all canceled subject matter in related applications, and amend claim 7 so that the claims hereafter read as follows:

1. (Previously Presented) A method for authenticating a user over a network, comprising the steps of:

providing an identification box at the local site of the user, and providing a central server at a remote site, with the identification box including a biometric reader, and with the identification box and the central server being connected over the network;

confirming the identity of the user to the central server, using the identification box;

sending a unique math table from the central server to the identification box, with the unique math table being stored at both the central server and the identification box;

measuring a first biometric parameter from the user with the biometric reader, and storing the first biometric parameter in encrypted form at the identification box and at the central server;

sending a user request for authentication from the identification box to the central server;

sending a random number from the central server to the identification box;

measuring a second biometric parameter from the user with the biometric reader;

encrypting the second biometric parameter;

comparing, at the identification box, the second encrypted biometric parameter with the previously-stored first encrypted biometric parameter;

operating on the random number, at the identification box, with the unique math table to create a first cryptogram when a positive match occurs between the first and second encrypted biometric parameters;

operating on the random number, at the central server, with the unique math table to create a second cryptogram;

sending the first cryptogram from the identification box to the central server;

comparing, at the central server, the first cryptogram with the second cryptogram; and

confirming the authenticity of the user when a positive match occurs between the first cryptogram and the second cryptogram.

2.-5. (Canceled)

6. (Previously Presented) A method for authenticating a user over a network as in claim 1 further comprising the step of allowing the user access to a second remote site if the first cryptogram matches the second cryptogram.

7. (Currently Amended) A method for authenticating a user over a network comprising the steps of:

providing an identification box at the local site of the user, and providing a central server at a remote site, with the identification box including a biometric reader, and with the identification box and the central server being connected over the network;

confirming the identity of the user to the central server, using the identification box;

sending a unique math table from the central server to the identification box, with the unique math table being stored at both the central server and the identification box;

measuring a first biometric parameter from the user with the biometric reader, and storing the first biometric parameter in encrypted form at the identification box and at the central server;

sending a user request for authentication from the identification box to the central server;

sending a first random number from the central server to the identification box;

measuring a second biometric parameter from the user with the biometric reader;

encrypting the second biometric parameter;

comparing, at the identification box, the second encrypted biometric parameter with the previously-stored first encrypted biometric parameter;

generating, at the identification box, a second random number when the first encrypted biometric parameter does not positively match the second encrypted biometric parameter;

operating on the second random number, at the identification box, with the unique math table to create a first cryptogram when a positive match fails to occur between said first and second encrypted biometric parameters,

operating on the first random number, at the central server, with the unique math table to create a second cryptogram;

sending the first cryptogram from the identification box to the central server;

comparing, at the central server, the first cryptogram with the second cryptogram; and

denying the authenticity of the user when there is no match ~~occurs~~ between the first cryptogram and the second cryptogram.

8. (Previously Presented) A method for authenticating a user over a network as in claim 7 further comprising the step of denying the user access to a second remote site if the first cryptogram does not match the second cryptogram.

9. (Cancelled)

10. (Previously Presented) A method according to claim 1 further comprising:

providing a second identification box at a second remote site, with the second identification box including a second biometric reader, and with the second identification box and the central server being connected over the network;

sending a user request for authentication from the second identification box to the central server;

sending the unique math table and the first encrypted biometric parameter from the central server to the second identification box;

sending a second random number from the central server to the second identification box;

measuring a third biometric parameter from the user with the second biometric reader;

encrypting the third biometric parameter;

comparing, at the second identification box, the third encrypted biometric parameter with the first encrypted biometric parameter;

operating on the second random number, at the second identification box, with the unique math table to create a third cryptogram when a positive match occurs between the first and third encrypted biometric parameters;

operating on the second random number, at the central server, with the unique math table to create a fourth cryptogram;

sending the third cryptogram from the second identification box to the central server;

comparing, at the central server, the third cryptogram with the fourth cryptogram; and

confirming the authenticity of the user when a positive match occurs between the third cryptogram and the fourth cryptogram.

11. (Canceled)